Пример оценки риска

написано Александр Астахов | 10 июня, 2023

В качестве примера, оценим величину информационного риска, связанного с хищением оборудования и (или) носителей информации собственными сотрудниками некой воображаемой организации (см. рис. 29). Для этого будем использовать откалиброванную выше качественную шкалу.

Сущность данной физической угрозы и способы ее осуществления известны каждому. Попытки хищения время от времени происходят во многих организациях, о чем могут свидетельствовать как личные наблюдения, так и доступная статистика. Регулярность осуществления данной угрозы обусловлена сравнительной простотой ее осуществления и склонностью некоторых людей к воровству. Недостаточный уровень лояльности персонала, отсутствие серьезных проверок кандидатов на работу, большое количество случайных и временных людей в штате компании – это те факторы, которые повышают вероятность попыток хищения в данной воображаемой организации.

Приведенные соображения позволяют оценить вероятность угрозы хищения оборудования и (или) носителей информации сотрудниками организации как Среднюю, со средней ожидаемой частотой реализации ~ 1 раз в год. При этом реальное количество попыток хищения согласно накопленной статистике может лежать, например, в диапазоне от 0,5 до 5 попыток в течении года.

Общий уровень уязвимостей, способствующих успешному осуществлению данной угрозы в нашей воображаемой организации, оценивается с учетом следующих факторов:

- не производится регистрация оборудования и носителей информации, выносимых за пределы организации
- не регламентированы правила работы в зонах безопасности, включая серверные комнаты, в которых размещается наиболее критичное оборудование и носители информации

С другой стороны, в организации могут приниматься определенные меры по противодействию угрозе хищения, включающие в себя, например:

- наличие политики, регламентирующей правила работы сотрудников с мобильными носителями информации
- наличие политики возврата оборудования, носителей информации и документов при увольнении сотрудников из организации
- контроль входа-выхода на ресепшене сотрудниками охраны в сочетании с видеонаблюдением
- наиболее критичное оборудование и носители конфиденциальной информации размещаются в зонах безопасности, доступ в которые ограничен

Взвешивая перечисленные выше уязвимости с одной стороны и механизмы контроля – с другой, мы можем прийти к выводу о том, что далеко не каждая попытка хищения из организации будет успешной, а лишь примерно половина их них. Это позволяет нам оценить суммарный уровень уязвимости как Средний, что примерно соответствует 50% вероятности успеха в случае реализации данной угрозы.

В качестве информационного актива, в отношении которого рассматривается угроза хищения, возьмем для примера проектную документацию организации. Хищение носителя с проектной документацией может привести к попаданию данной информации к конкурентам и, как следствие, потере конкурентных преимуществ для организации. Кроме этого, попадание проектных документов в открытый доступ, может привести к нарушению конфиденциальности информации третьих лиц, являющихся клиентами данной организации. В результате придется уплачивать штрафы по искам этих третьих лиц на основании заключенных с ними соглашений о конфиденциальности. Помимо этого, репутации организации в данном случае будет нанесет ощутимый урон, который выльется, в конечном счете, в сокращении числа клиентов, заказов и

уменьшении выручки.

Предположим, что по результатам обсуждения и анализа данных предполагаемых последствий с менеджерами организации ценность проектной документации была оценена по уровню 2, что соответствует среднему ущербу в 4 млн. руб. (см. раздел «Калибровка шкалы оценки рисков» выше). Реальный ожидаемый ущерб при этом может находиться, например, в диапазоне от 3 до 5 млн. руб.

Среднегодовой ущерб (ALE) рассчитывается по формуле:

ALE = [размер ущерба] × [количество инцидентов в год] × [вероятность успешной реализации угрозы].

В нашем случае, ожидаемый среднегодовой ущерб от физического хищения проектной документации, вычисляется следующим образом:

ALE ~ 4 млн. × 1 × 0,5 = 2 млн. руб.

Это средний уровень риска, равный 4, согласно откалиброванной выше качественной шкале. Полученное значение ALEне является точным и всегда обозначает лишь порядок величины. Реальное ALEможет лежать в диапазоне от 0,3 до 3 млн. руб.

Из приведенного примера видно, что наша оценка риска не претендует на то, чтобы быть точной. Реально нас интересует лишь диапазон, в который попадает величина ALE. На практике этого вполне достаточно для ранжирования рисков и принятия экономически обоснованных решений по их обработке.